(U) Putting the 'Gap' in AIRGAP

FROM: Charlie Speight
Internet Program Manager (IT Directorate)
Run Date: 06/03/2005

Security issues regarding the non-attribution internet program... (U//FOUO)

(U//FOUO) A SID *today* reader recently wrote in with a question about NSA's AIRGAP (non-attribution Internet access) program. He had heard that the Agency uses a single IP address for the entire Agency that changes only about once a year, due to "lack of funding." There was concern that "it would be easy for the enemy to learn our IP address and see what we are researching every day. Or worse, create rules based on that IP address that show us false content (denial and deception)." Let me address this issue.

(U//FOUO) The issue of IP addresses used by the OSIS-owned non-attributable firewall is an old one and has often been misrepresented.

(C) What we at NSA call "AIRGAP" is actually a commercial firewall owned by OSIS (a component of the Intelink Management Office) and run by one of the world's largest ISPs*. NSA piloted this firewall in 1997-98 for OSIS to test its viability for the entire Intelligence Community. That initial effort -- the brainchild of [redacted] -- was referred to here as "MIMIR." When it went operational, NSA (and only NSA) called this new service "AIRGAP."

(U//FOUO) All of the Intelligence Community (IC) has access to and uses this firewall. Thus, we are tenants and do not control the protocols of the firewall except to make requests or offer suggestions. Early on, NSA saw the need for more than one IP address believing it much more "non-attributable" to have multiple addresses to insure greater obscurity. OSIS agreed to have the ISP add more IP addresses although they disagreed with the necessity. Despite the change, occasionally we find that the ISP reverts to one address, or does not effectively rotate those assigned. On other occasions, NSA has requested other changes, such as turning off http-referrer, which OSIS has also accommodated. Unfortunately, the changes didn't always "stick" and the ISP would revert to original settings. When that happened, it was usually this Agency that pointed to the problem and asked to have the changes reinstated.

(C) Keep in mind that the firewall and its IP address(es) are not used just by/for NSA, but for the entire Intelligence Community. Because of that, a compromise or attempt by a webmaster to isolate the use of a particular address used by this firewall will not necessarily reveal NSA users. In fact, the greater security concern is inappropriate use of AIRGAP by users. Despite rules and warnings to the contrary, all too frequently users will use AIRGAP for registering on web sites or for services, logging into other sites and services and even ordering personal items from on-line vendors. By doing so, these users reveal information about themselves and, potentially, other users on the network. So much for "non-attribution."

(U//FOUO) So, the contention that there is only one IP is incorrect, though, practically, that may occasionally be the effect. As for the reason being a "lack of funding," that is untrue.

(U//FOUO) As the largest volume user of this non-attributable firewall (by far!), NSA has come to rely on it much more than have others in the IC. As a result, our concerns about its operation exceed those of OSIS and our reliance on it has grown exponentially.

(C) So... what do we do? Before the end of this fiscal year, these will be moot points. With the advent of the new unclassified network -- OUTPARKS (see link below) -- **NSA will begin its own non-attributable (AIRGAP) service.** NSA will determine the protocols by which the firewall will operate. Among those protocols will be the use of multiple (over 200, I've been told), randomly generated IP addresses. And, as is currently practiced by the OSIS firewall,

those IP addresses will be registered to one of the world's largest ISPs -- not NSA, the Intelligence Community or even the government.

(C) We are acquiring our own service for several reasons. Control over the operation of the firewall is essential. We've found that by being a tenant on someone else's system, we often don't share the same security interests or sensitivities about bandwidth, down time or other operational requirements. But another reality is that we have outgrown the OSIS approach and are using "AIRGAP" for reasons and in volumes not intended in its formation. The word "AIRGAP" has become part of the NSA lexicon, so much so that when it was suggested that the new, NSA-owned non-attributable access be given a new name, the idea was rejected because of the familiarity users have with the term.

(U//FOUO) For more on professional and personal security practices on the Internet, get Robyn Winder's superb book "Untangling the Web" (link below). This Intelligence Community standard is now available in hardcopy and CD Rom at the Main Library (OPS1, Room 1S042) and in the R&E Library (Room R1C075). It is also available on-line on NSANet, OSIS, Intelink and SIPRnet. For more information on the Internet at NSA, use the URN "go internet" on NSANet.

OUTPARKS: http://[redacted]
UNTANGLING THE WEB: http[redacted]

*(U) ISP = Internet Service Provider
